.TENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
DAVID R. METZGER
SONNENSCHEIN NATH & ROSENTHAL
POST OFFICE BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606

PCT

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

(PCT Rule 43*bis*.1)

Date of mailing (day/month/year)	**15 APR 2005**

FOR FURTHER ACTION
See paragraph 2 below

Applicant's or agent's file reference		
8758PCT		

International application No.	International filing date (day/month/year)	Priority date (day/month/year)
PCT/US04/21621	07 July 2004 (07.07.2004)	07 July 2003 (07.07.2003)

International Patent Classification (IPC) or both national classification and IPC

IPC(7): G06F 12/14 and US Cl.: 713/185

Applicant

CRYPTOGRAPHY RESEARCH

---

1. This opinion contains indications relating to the following items:

☒ Box No. I   Basis of the opinion

☐ Box No. II   Priority

☐ Box No. III   Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

☒ Box No. IV   Lack of unity of invention

☒ Box No. V   Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

☐ Box No. VI   Certain documents cited

☐ Box No. VII   Certain defects in the international application

☐ Box No. VIII   Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority data, whichever expires later.

For further options, see Form PCT/ISA/220.

presumably by July 15, 2005

May 7, 2005

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Authorized officer *Michelle R. Zion*
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450	Andrew Caldwell
Facsimile No. (703) 305-3230	Telephone No. 305-3900

Form PCT/ISA/237 (cover sheet) (January 2004)

CC = J. Yang

Box No. I Basis of this opinion

1. With regard to the language, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ This opinion has been established on the basis of a translation from the original language into the following language _____, which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any nucleotide and/or amino acid sequence disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material

      ☐ a sequence listing

      ☐ table(s) related to the sequence listing

   b. format of material

      ☐ in written format

      ☐ in computer readable form

   c. time of filing/furnishing

      ☐ contained in international application as filed.

      ☐ filed together with the international application in computer readable form.

      ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

International app.._ation No.

PCT/US04/21621

Box No. IV Lack of unity of invention

1. ☒ In response to the invitation (Form PCT/ISA/206) to pay ~~additional~~ *prescribed* fees the applicant has:

    ☒ paid additional fees

    ☐ paid additional fees under protest

    ☐ not paid additional fees

2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rule 13.1, 13.2 and 13.3 is

    ☐ complied with

    ☒ not complied with for the following reasons:

    See the lack of unity section of the International Search Report(Form PCT/ISA/210)

4. Consequently, this opinion has been established in respect of the following parts of the international application:

    ☐ all parts.

    ☒ the parts relating to claims Nos. 1-4 and 11

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-4, 11	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-4, 11	NO
Industrial applicability (IA)	Claims 1-4, 11	YES
	Claims NONE	NO

2. Citations and explanations:

Claims 1-4, and 11 lack novelty under PCT Article 33(2) as being anticipated by Schneck et al., US 6,314,409.

As for claim 1, Schneck teaches a method for regulating access to non-volatile digital storage contained in a device executing instructions in a Touring-complete interpreter (abstract), said method comprising: Receiving a request from said instructions being executed (fig. 11, items S1104, S1106, S1110), wherein said request specifies a portion of said storage for which access is requested (col. 11 Table 1), a plurality of additional executable instructions (col. 11 Table 1), applying a cryptographic hash function to said additional executable instructions to obtain a hash value (Col. 11 Table 1: "Authentication Hash"), Authentication said hash value (fig. 11 item S1110 "Integrity Checker"), and provided that said authentication is successful, enabling access to said requested portion of said storage while executing additional executable instructions (Fig. 12 item S1212, col. 7 lines 41-48, col. 15 lines 30-40, col. 19 lines 61-67, col. 20 lines 1-4).

As for Claim 2, Schneck teaches a step of authenticating that comprises comparing a hash value with a hash value stored in non-volatile memory (Col. 11 Table 1 "Authentication Hash", fig. 11 item S1110: "Integrity Checker", col. 20 lines 30-35).

As for claim 3 Schneck teaches a step of authenticating that comprises verifying a digital signature provided by said instructions being verified (col. 31 lines 20-25).

As for claim 4, Schneck does not explicitly teach the use of a pointer to additional executable instructions in memory accessible by said instructions being executed and contained in said device. However such a feature is inherent in the system of Schneck. For example col. 7 lines 21-25 teach an encrypted rule set stored in non-volatile memory along with content data and where the content data is accessible on in accordance with the rules. Col. 11 lines 1-3 teach header information that is navigated in accordance with a rule set.

As for claim 11, Schneck teaches an automated method for determining whether to allow a portion of software stored in a computer-readable memory to access a portion of non-volatile memory (abstract), the method comprising receiving a reference to said software (fig. 3), computing a cryptographic hash of said software portion (fig. 3 item 128: "Authentication Hash"), comparing said computed cryptographic hash with a value stored in said non-volatile memory (Fig. 11 item S1110), when said computed cryptographic has matches said stored value, allowing said software portion to access said non-volatile memory portion and when said computed cryptographic hash does not match said stored value, not allowing said software portion access to said non-volatile memory (Fig. 11 Item S1110, S1112, S1127).